RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: IMT-T02

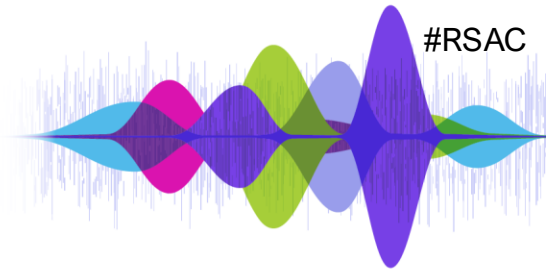
Your Policies and Procedures Were Perfect, Still, You Got Hacked. Why?

Michel Coene

Director CSIRT services
NVISO Security
linkedin.com/in/coenemichel/

Vincent Defrenne

Director Cyber Strategy services
NVISO Security
linkedin.com/in/vincentdefrenne



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

An introduction to Critical Attack Success Points (CASPs)

Recognize this?

My policies and procedures were perfect…

And Still, I Got Hacked.

Why?

Incident at customer X (december 2024)

We got called after…
Paid out 350k€ worth of fraudulent invoices

They told us…
“But we had all the necessary controls: we’re ISO27001 !”

And the investigation showed that…
- Implemented MFA but with push notifications only, which was abused through MFA bombing
- Implemented basic payment verification procedures, but were not verifying new bank accounts through a secondary channel

Conclusion
Controls implementation was too superficial, not threat-based.

Recognize this?

My policies and procedures were perfect…

And Still, I Got Hacked.

Why?

Incident at customer Y (January 2025)

We got called after…
Full ransomware deployment and loss of backups

They told us…
"But we had all the necessary controls : we patched regularly!"

And the investigation showed that…

- Patching policy ensured 6-weekly patching of Fortinet firewalls. But underlying vulnerabilities were not considered, and the 6-weeks window was enough to compromise the firewall
- Strong password policy, but password re-use
- "We have MFA": yes, but only for M365

Conclusion
Controls implementation was too superficial, not threat-based.

But also…

Customer A

We've implemented the NIST CSF

Most controls are now in place

And we even test their effectiveness

… but I'm not sure we're testing the ***right*** controls that will ***really*** block typical cyber attacks.

But also…
Customer B

We perform regular red team tests

We organize tabletop crisis exercises 3x/year

We implemented Caldera for BAS

… but I'm not sure we're testing the ***right*** controls that will ***really*** block typical cyber attacks.

How it all started…

Let's start with the most likely ***threats***

Define the most probable ***attack scenarios***

And break it down into a ***kill chain***

We could then identify the ***steps*** in the kill chain that are ***crucial*** to the success of an attack.

And verify those ***Critical Attack Success Points***.

Or CASPs

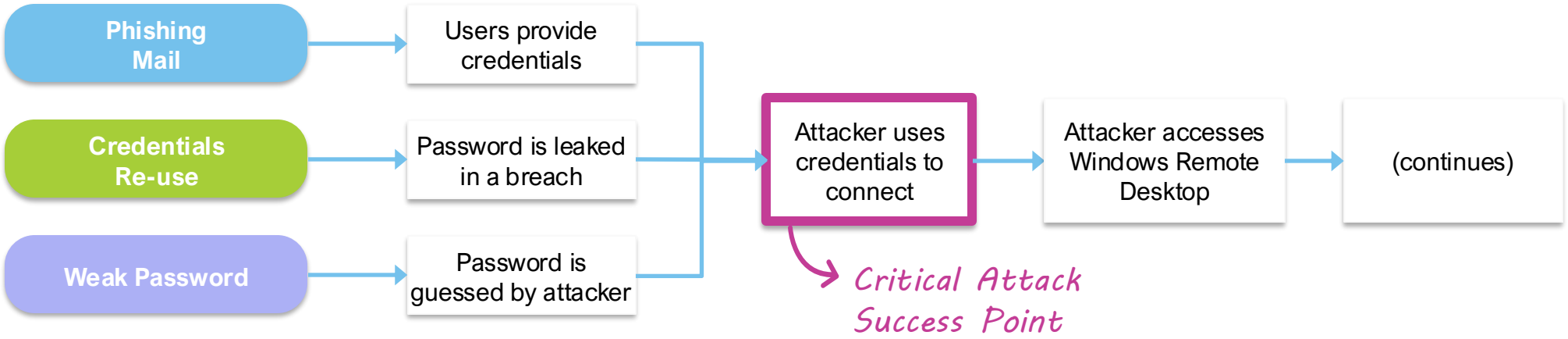
Introducing CASPs

Critical Attack Success Points

What are CASPs?

- A CASP is one step in the attack kill chain that is essential for the attacker to progress … and therefore, it is also a single point where an attack can be stopped
- It is typically a step in which different attack paths converge, and which is crucial to the attacker to continue its attack. It's a single 'make or break' point for the attack.
- It can consist of technical or procedural controls; it can consist of IT or business control

Example: looking at a specific step, i.e. use of stolen credentials



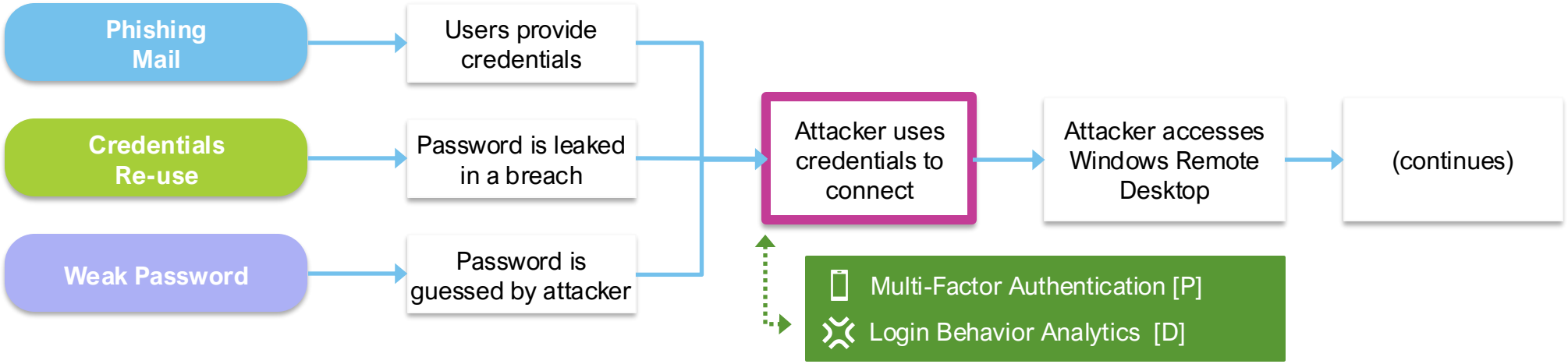
Introducing CASPs

Critical Attack Success Points

Why focus on CASPs?

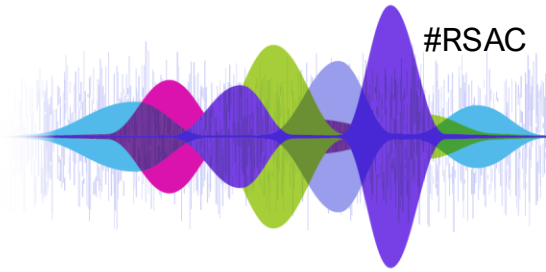
- The CASPs represent a key step in the attack:
  - If that step is effectively blocked, the attack can be stopped ▸ controls to **prevent**
  - If that step is effectively detected, the attack can be stopped ▸ controls to **detect, respond** and even **recover**
- So, the CASPs help focus on ***controls that can really stop an attack.***

Example: looking at a specific step, i.e. use of stolen credentials



Introducing CASPs

Critical Attack Success Points



So, what are we solving with CASPs?

- Identifying CASPs is an excuse to do threat modelling with a focus: ***finding controls you are most concerned about.***

- The CASPs represent a key step in the attack. As such:
  - If that step is effectively **blocked**, the attack can be **stopped**
    - controls to **PREVENT**
  - If that step is effectively **detected**, the attack can be **stopped**
    - controls to **DETECT and RESPOND**
  - If that step is successful, rapid recovery will be key to reduce business impacts
    - controls to **RECOVER**

- So, the CASPs help focus on ***controls that can really stop an attack.***

Introducing CASPs

Critical Attack Success Points

How to identify CASPs?

For a specific attack scenario, we draw the attack kill chain and identify single steps that are crucial to the continuation of the attack (“make or break points”):

These are the Critical Attack Success Points (CASPs)

1. Threat Scenario

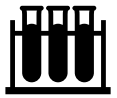
Determine key threat scenarios for your organization

2. Kill Chain

For a selected threat scenario, define the attack kill chain

3. CASPs

Visually identify key steps where the attack path converges



4. Controls

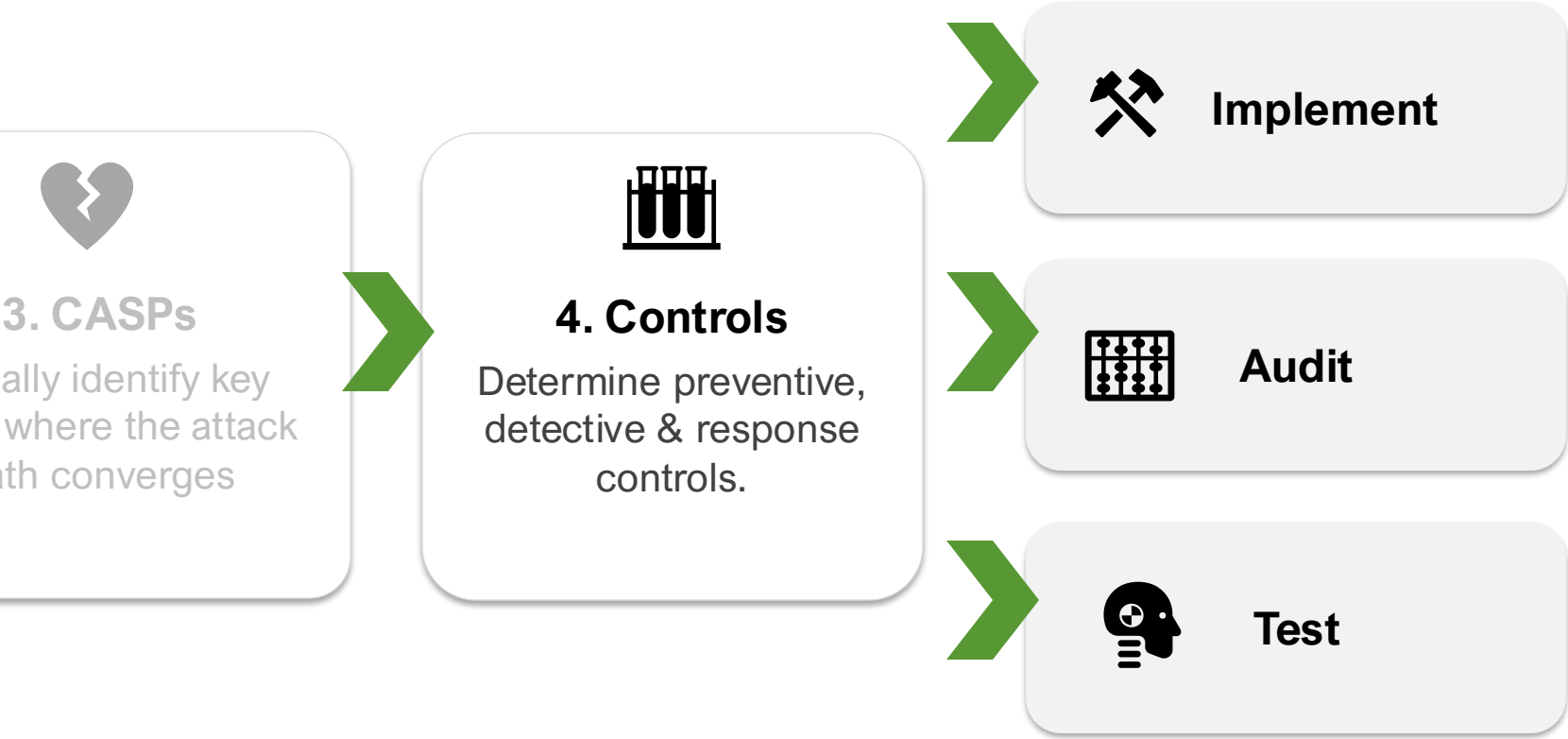
Determine preventive, detective & response controls.

Introducing CASPs

Critical Attack Success Points

How to leverage CASPs?

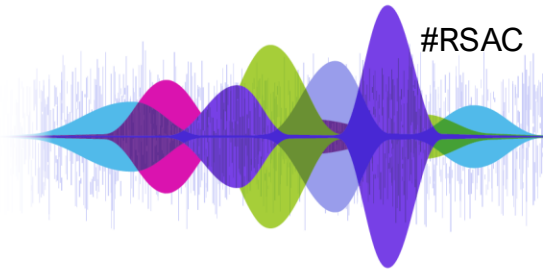
- We typically leverage those for the following three purposes



Example:
We used it to define the '25-'27 cyber strategy focused on "most impacting controls" for top 10 threat scenarios.

Example:
We organized tabletop exercises with counter-CASP control owners to identify areas for improvement.

Example:
We leverage CASPs in defining scope or scenario for Red Team testing.



In the remainder of this presentation, we will…

1. Provide two examples of how to **identify** CASPs
2. Provide a two examples of how to **use** CASPs
3. Share a few **other use cases** for CASPs

RSAC 2025 Conference

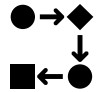
Identifying CASPs

Devising the kill chain and identifying the CASPs

Identifying CASPs

1. Threat Scenario

Determine key threat scenarios for your organization

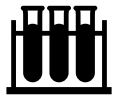


2. Kill Chain

For a selected threat scenario, define the attack kill chain

3. CASPs

Visually identify key steps where the attack path converges



4. Controls

Determine preventive, detective & response controls.

Identifying CASPs

1. Threat Scenario

Determine key threat scenarios for your organization

2. Kill Chain

For a selected threat scenario, define the attack kill chain

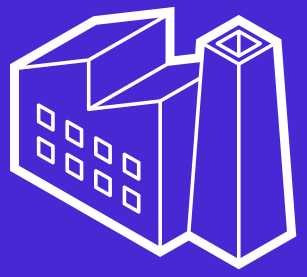
3. CASPs

Visually identify key steps where the attack path converges

4. Controls

Determine preventive, detective & response controls.

Identifying CASPs
1. Threat Scenario



Manufacturing company

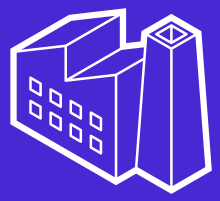
Not part of a governmental or military supply chain.

Not producing dual use goods.

Who would target us?

And **Why**?

Identifying CASPs
1. Threat Scenario



Who would target us?

And **Why**?

Initial Access Techniques

Phishing
Top Initial Access Technique for the 2nd Year Running

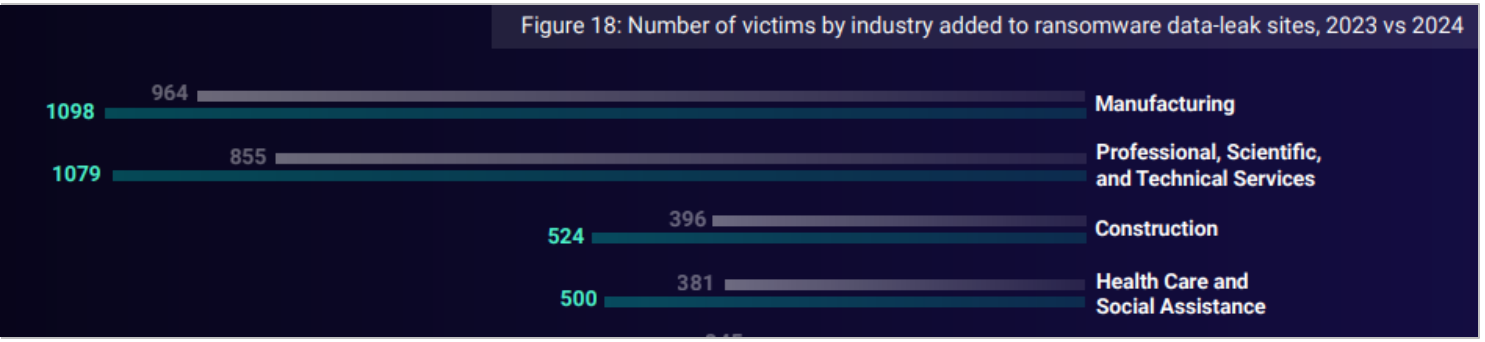
30%
Of Phishing Messages Involved Credential Harvesters

1 in 4
Active Intrusions Started with Exploitation of Public-Facing Applications

45%
Of Hands-on-Keyboard Intrusions Began with Abuse of External Remote Services Like VPNs

100%
Of Deployed MFA Controls Bypassed via Session Hijacking in Successful Business Email Compromise (BEC) Attacks

Source: Reliaquest



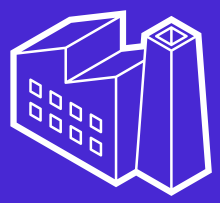
Source: Reliaquest

Manufacturing
(NAICS 31–33)

Frequency	2,305 incidents, 849 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 83% of breaches
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Personal (58%), Other (40%), Credentials (28%), Internal (25%) (breaches)
What is the same?	Two of the top patterns from last year are still in place. Financial motivation continues to be the driver behind most attacks.
Summary	Manufacturing has seen an increase in Error-related breaches. The installation of malware after hacking in via the Use of stolen credentials is also somewhat commonplace.

Source: 2024 Verizon DBIR report

Identifying CASPs
1. Threat Scenario



Who would target us?

And **Why**?

Scenarios are then identified, and inherent and residual risk are evaluated based on residual probability and residual impact.

This example, conclusion could include:

- *Threat Scenario D*
  Compromised e-mail results in **fraudulent financial transactions** (aka. Business Email Compromise (BEC))
- *Threat Scenario E*
  Phishing results in **fraudulent financial transactions** (aka. BEC)
- *Threat Scenario F*
  Vishing or other Social Engineering results in **fraudulent financial transactions** (aka. BEC)
- *Threat Scenario M*
  Stolen or guessed credentials lead to successful **Ransomware attack**
- *Threat Scenario N*
  Exploit of vulnerable web-facing system leads to successful **Ransomware attack**

Identifying CASPs

1. Threat Scenario

Determine key threat scenarios for your organization

2. Kill Chain

For a selected threat scenario, define the attack kill chain

3. CASPs

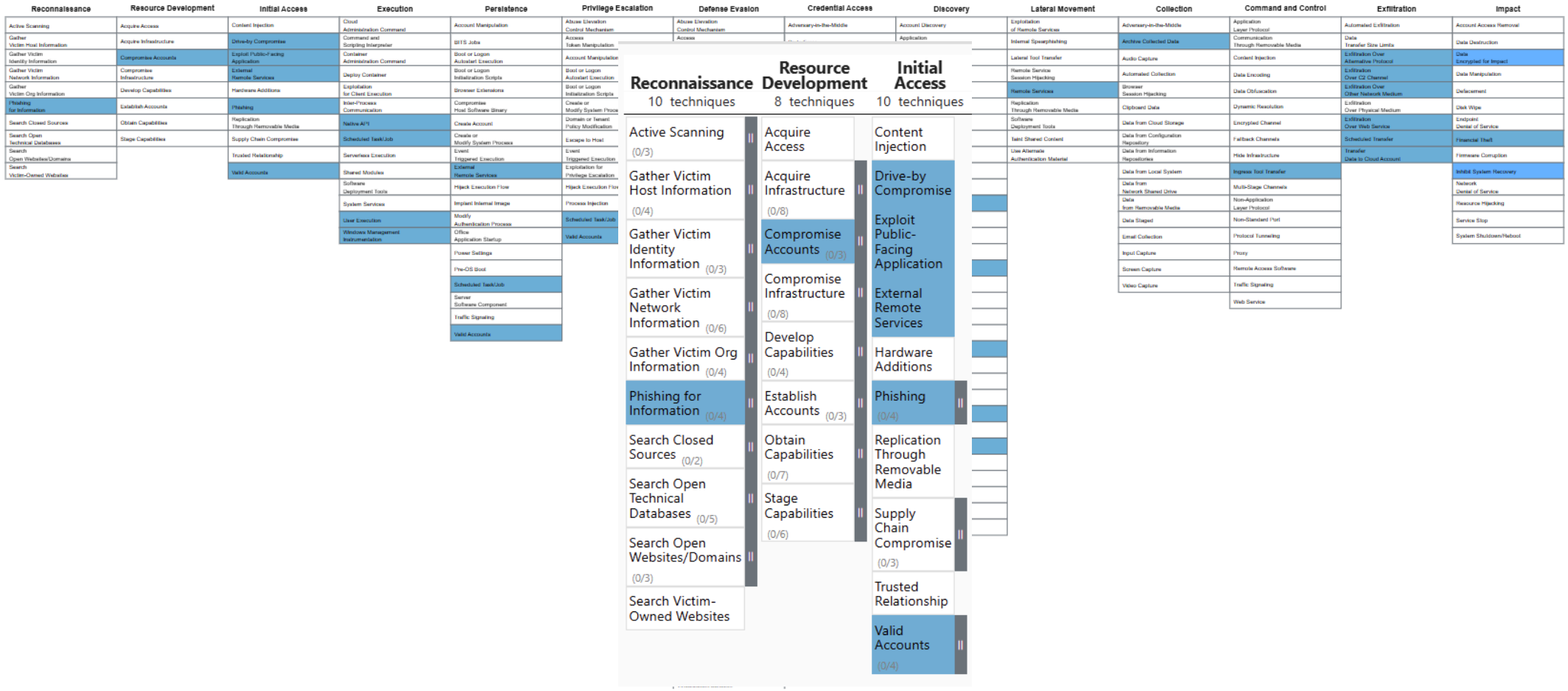
Visually identify key steps where the attack path converges

4. Controls

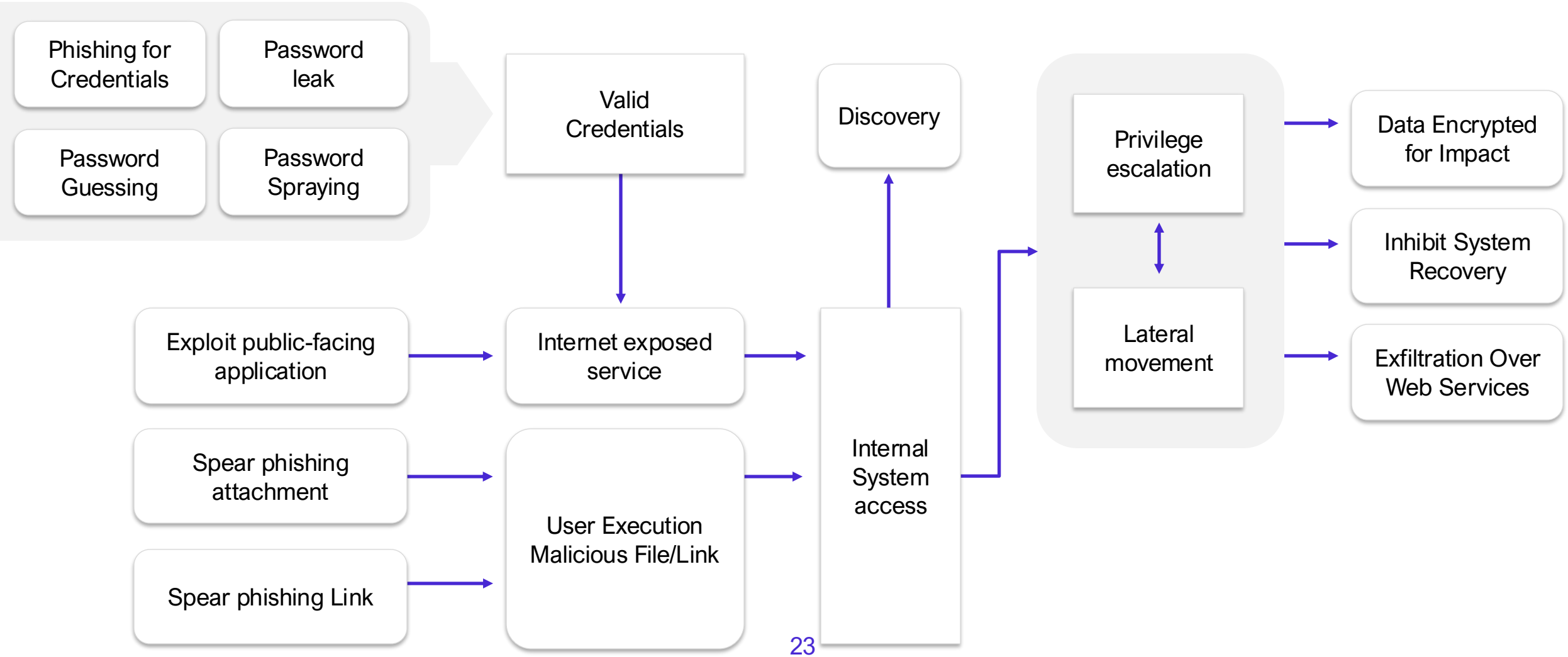
Determine preventive, detective & response controls.

Identifying CASPs
2. Kill Chain for a ransomware scenario

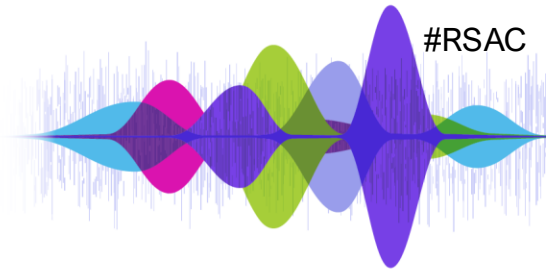
Example: MITRE ATT&CK matrix, highlighting tactics used by ransomware actors targeting the manufacturing industry



Identifying CASPs
2. Kill Chain for a ransomware scenario



Identifying CASPs



1. Threat Scenario

Determine key threat scenarios for your organization

2. Kill Chain

For a selected threat scenario, define the attack kill chain

3. CASPs

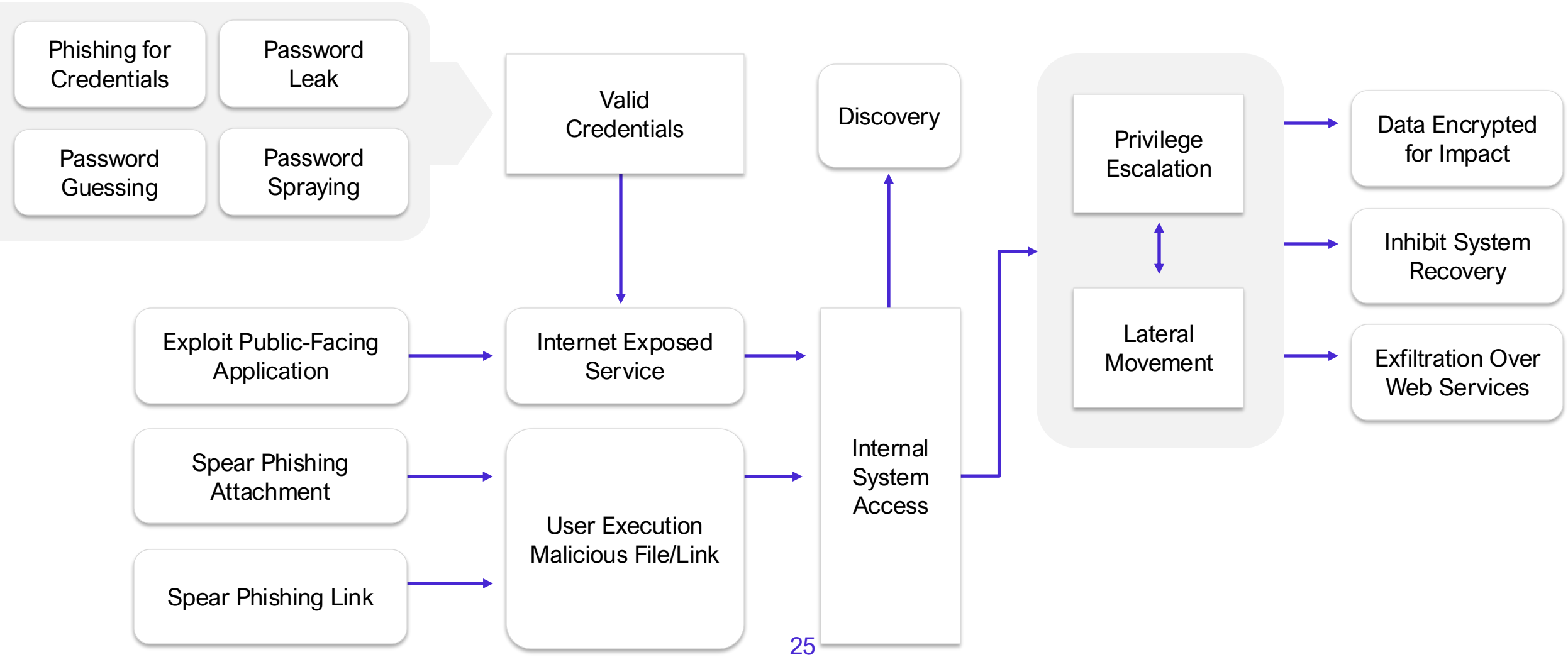
Visually identify key steps where the attack path converges

4. Controls

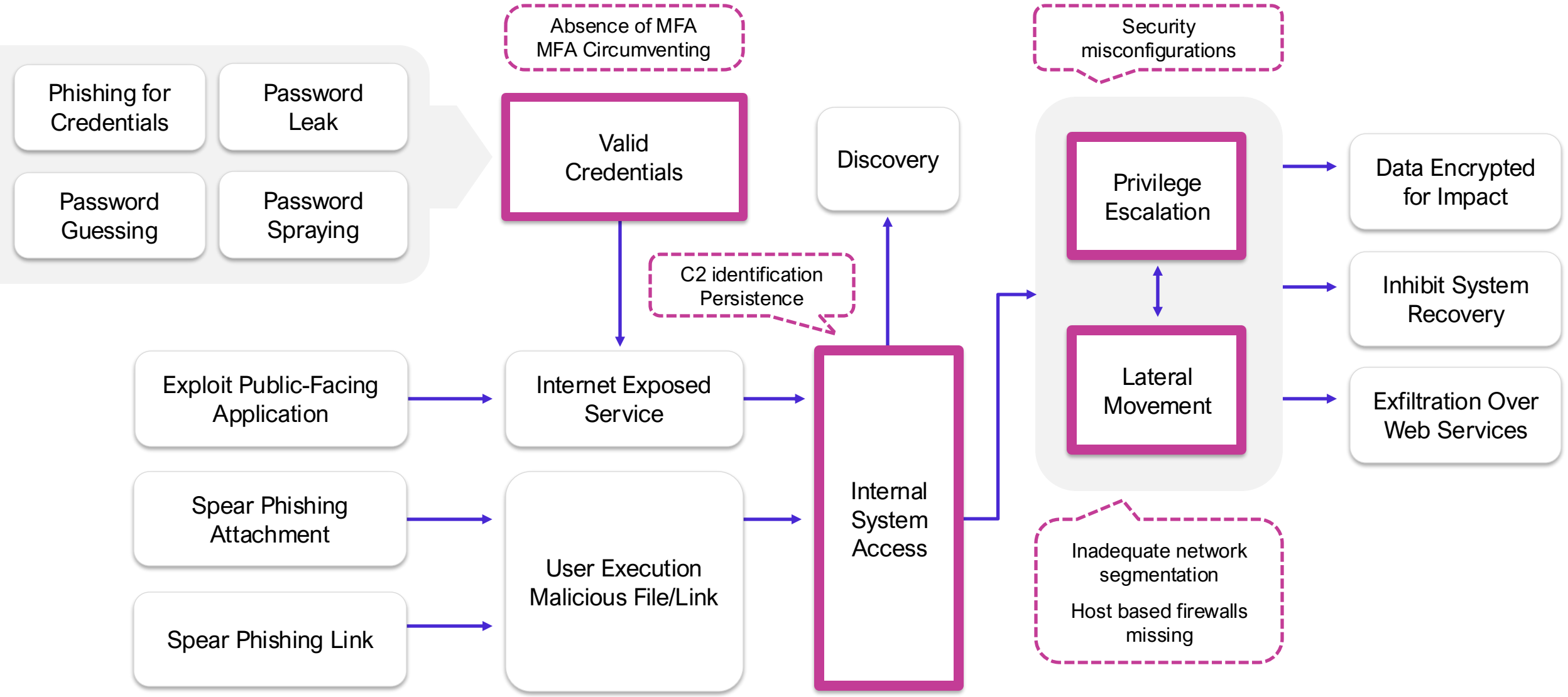
Determine preventive, detective & response controls.

RSAC 2025 Conference

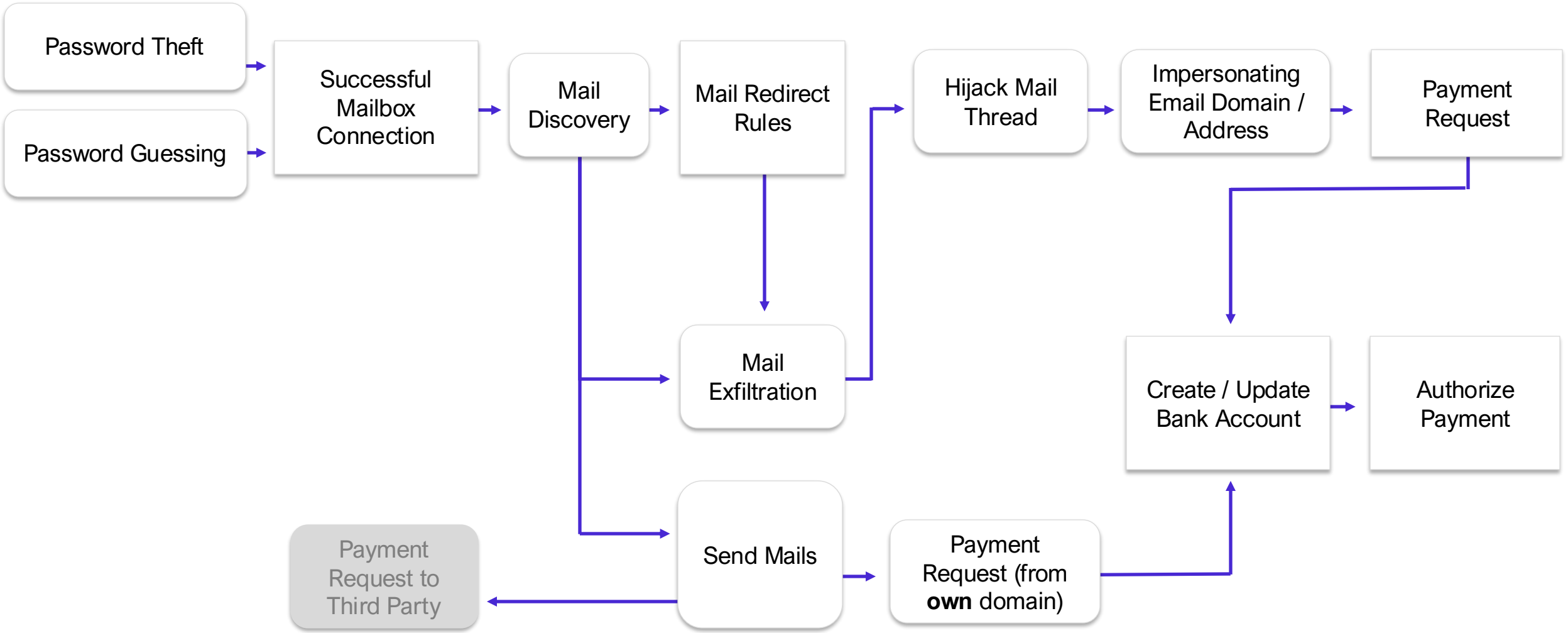
Identifying CASPs
3. Identifying CASPs for a ransomware scenario



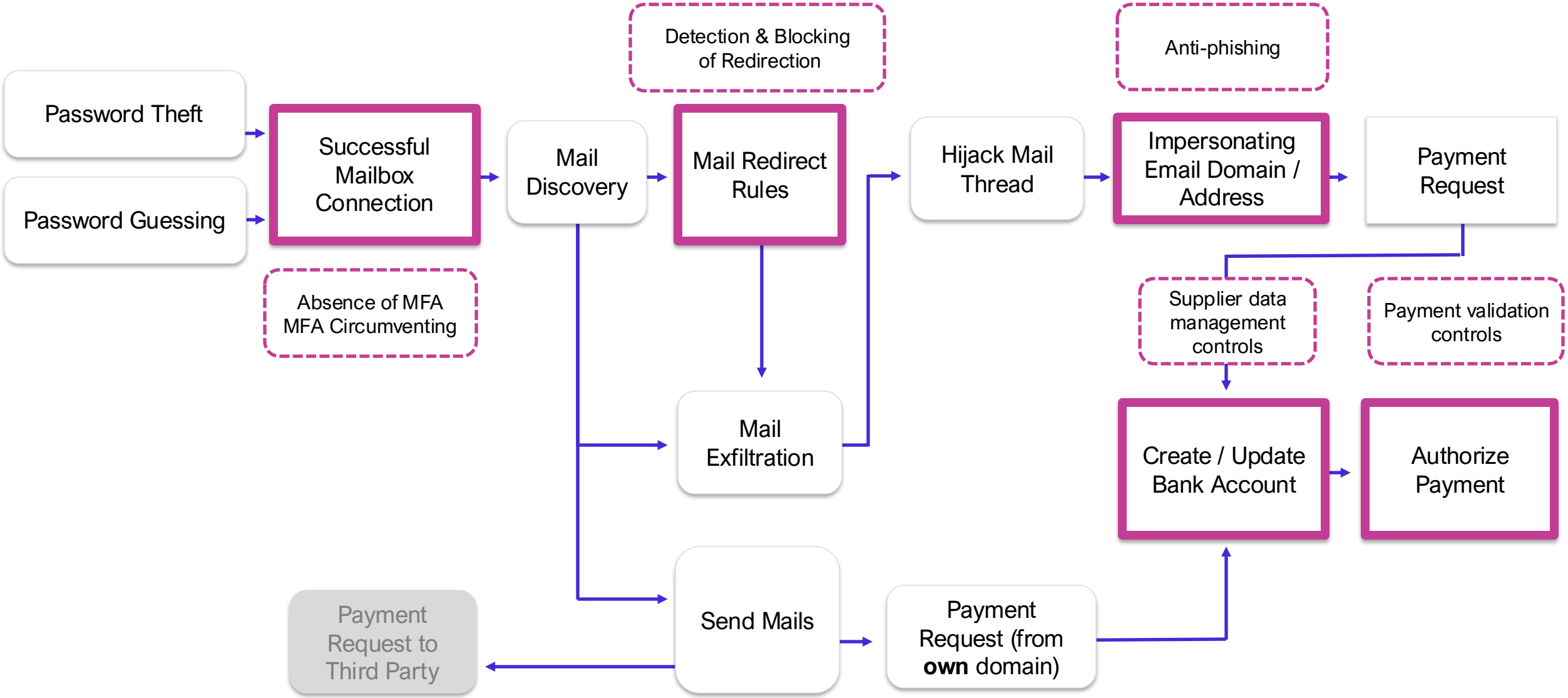
Identifying CASPs
3. Identifying CASPs for a ransomware scenario



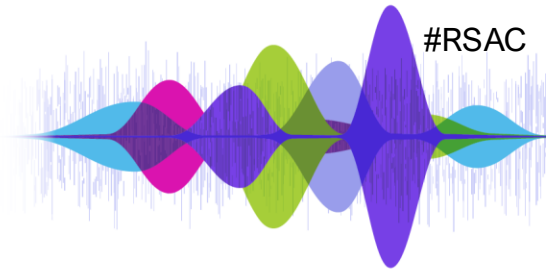
Identifying CASPs
Another example: Business Email Compromise (BEC)



Identifying CASPs
Another example: Business Email Compromise (BEC)



Identifying CASPs
… and now, let's use them



1. Threat Scenario

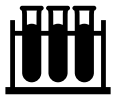
Determine key threat scenarios for your organization

2. Kill Chain

For a selected threat scenario, define the attack kill chain

3. CASPs

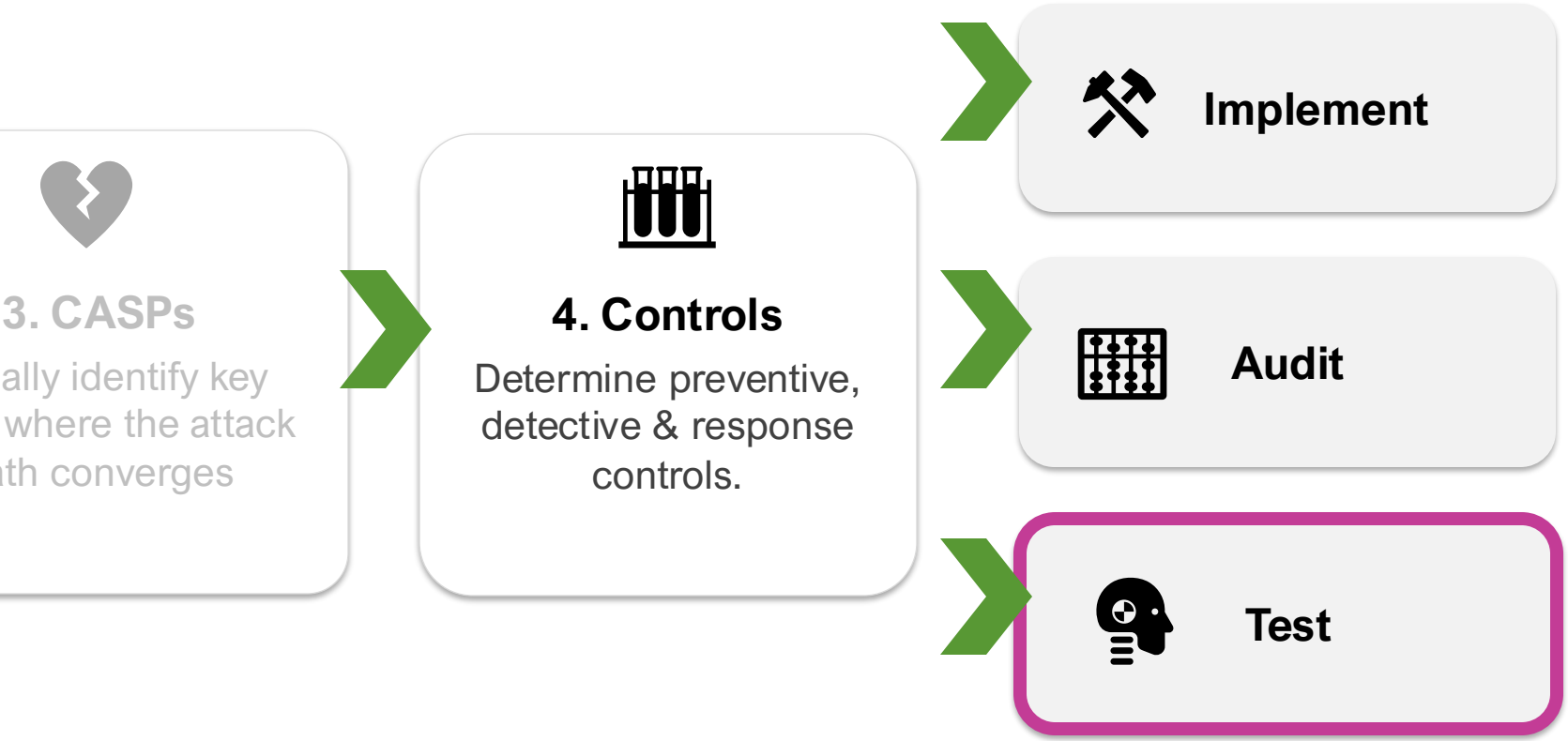
Visually identify key steps where the attack path converges



4. Controls

Determine preventive, detective & response controls.

Identifying CASPs
… and now, let's use them

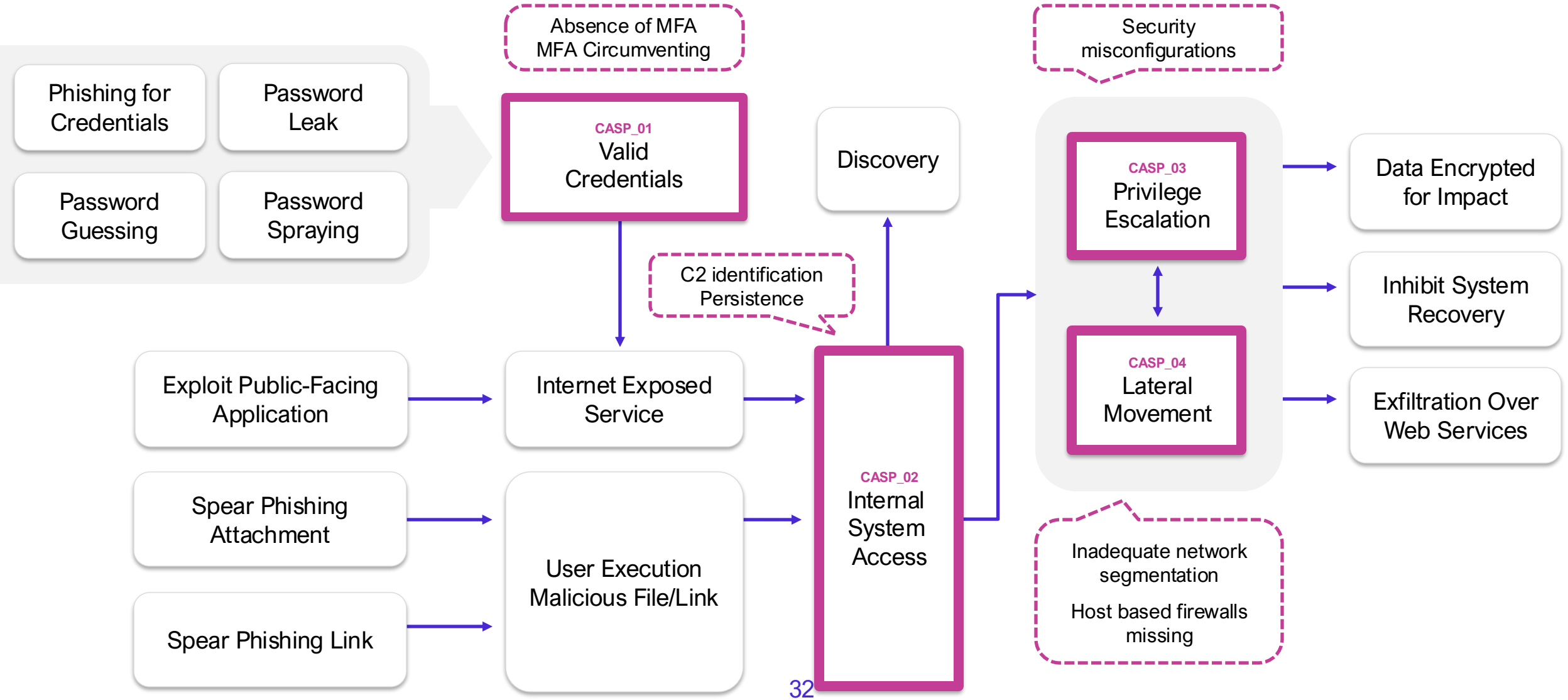


RSAC 2025 Conference

Using CASPs

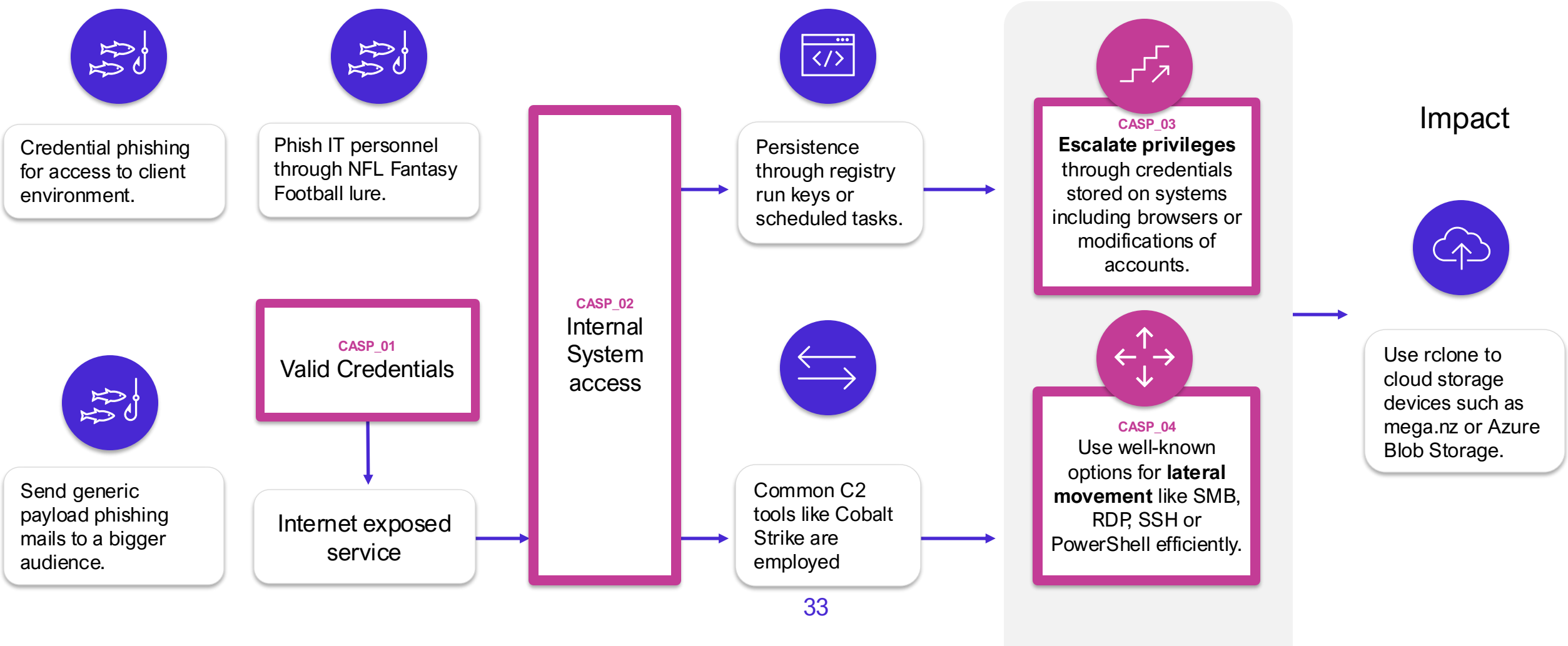
Example 1: Using CASPs to steer Red Team Testing scope

Using CASPs in Red Teaming
Ransomware

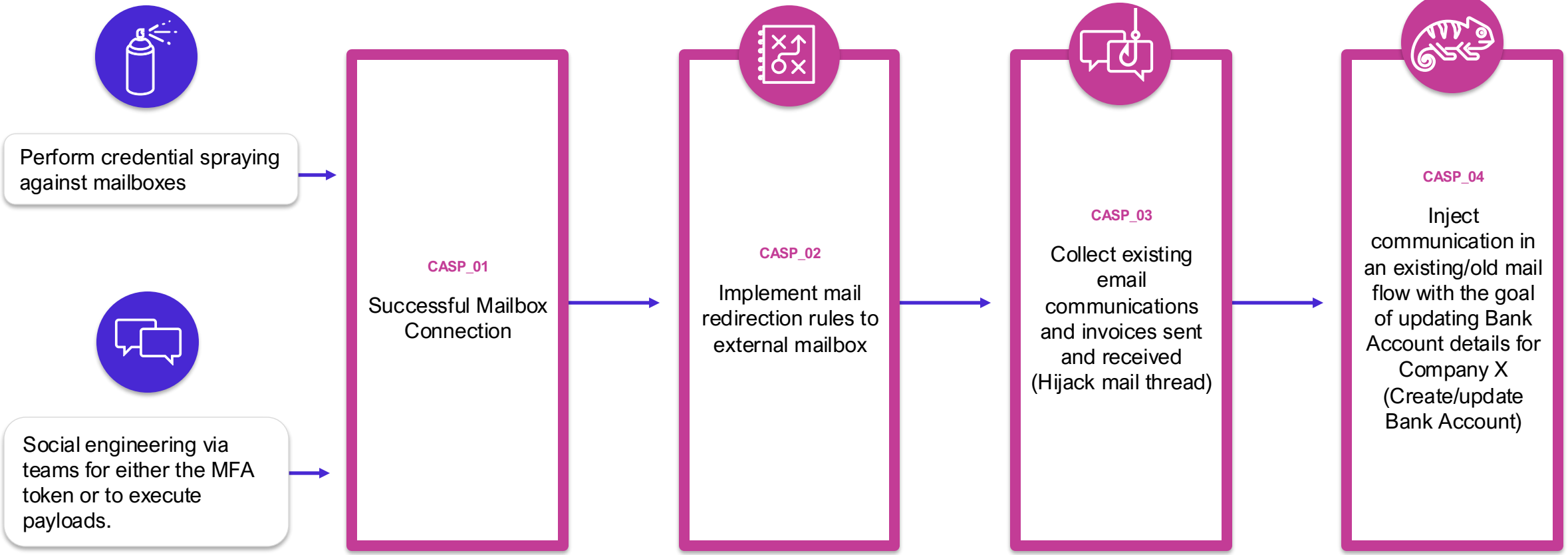


Using CASPs in Red Teaming
Ransomware

Positioning those CASPs into a red team testing scenario


Credential phishing for access to client environment.
Phish IT personnel through NFL Fantasy Football lure.
Send generic payload phishing mails to a bigger audience.
CASP_01
Valid Credentials
Internet exposed service
CASP_02
Internal System access
Persistence through registry run keys or scheduled tasks.
Common C2 tools like Cobalt Strike are employed
CASP_03
Escalate privileges through credentials stored on systems including browsers or modifications of accounts.
CASP_04
Use well-known options for lateral movement like SMB, RDP, SSH or PowerShell efficiently.
Impact
Use rclone to cloud storage devices such as mega.nz or Azure Blob Storage.

Using CASPs in Red Teaming
BEC


Perform credential spraying against mailboxes
Social engineering via teams for either the MFA token or to execute payloads.
CASP_01
Successful Mailbox Connection
CASP_02
Implement mail redirection rules to external mailbox
CASP_03
Collect existing email communications and invoices sent and received (Hijack mail thread)
CASP_04
Inject communication in an existing/old mail flow with the goal of updating Bank Account details for Company X (Create/update Bank Account)

Using CASPs in Red Teaming
Ransomware

You can also keep it simple !

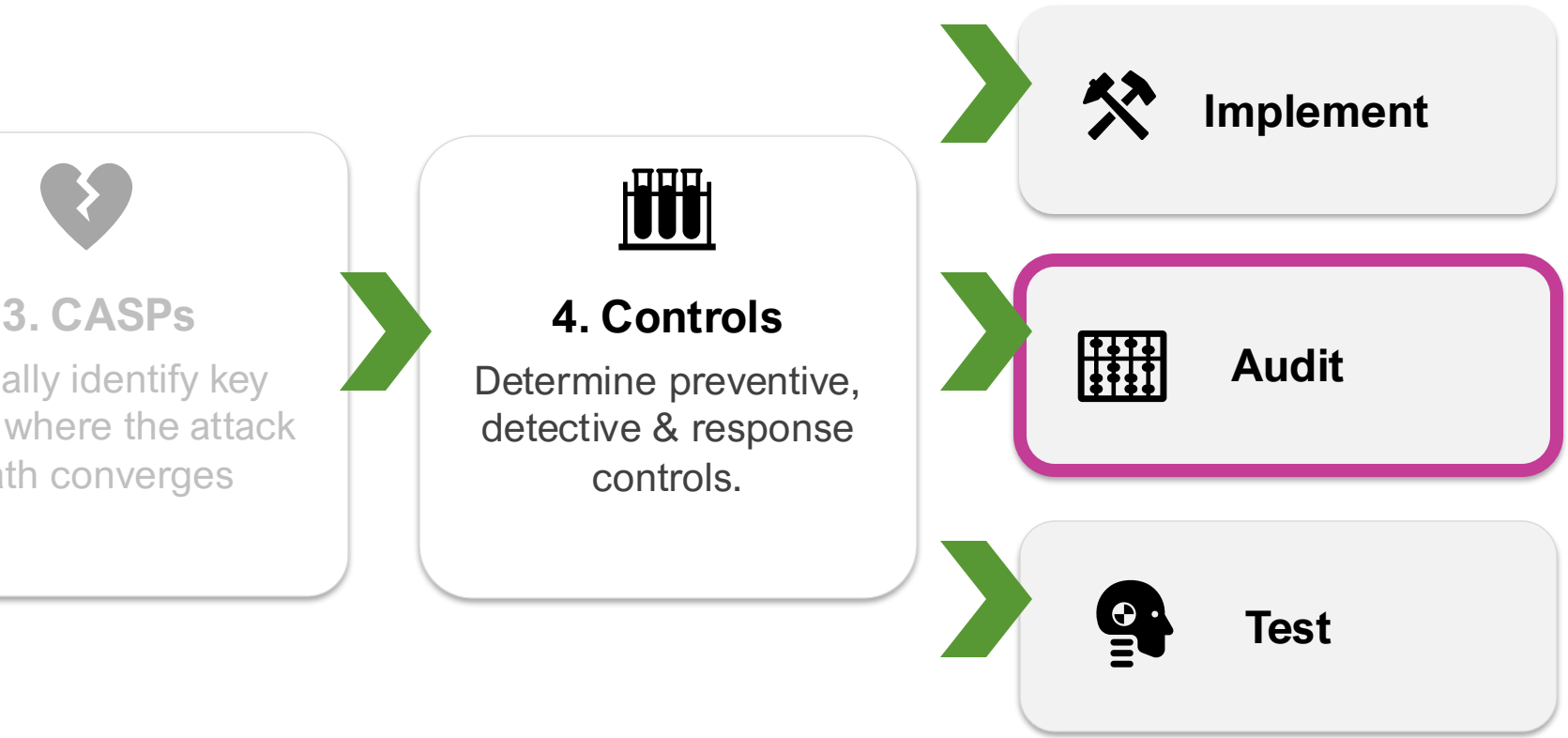
Alert helpdesk and handover infected computer
Escalation from L1 helpdesk towards L2 helpdesk
Ransomware infected computer
L1 Helpdesk
L2 Helpdesk

RSAC 2025 Conference

Using CASPs

Example 2: Using tabletop exercises to evaluate & improve CASP-countering controls

Using CASPs to audit key controls



Using CASPs to audit key controls

Using CASPs to audit key controls

Using tabletop exercises to audit CASPs

Our Goals

1. Identify **controls in place** to Prevent, Detect and Respond to CASP
2. Evaluate **adequacy** of these controls
3. Determine if **additional controls** are required / controls are **missing**
4. Stay away from **boring interviews**

Our Approach

1. Use **tabletop exercise techniques** for an interactive experience
2. Embed an **evaluation** of controls & reflection on **missing controls** into the exercise

Using CASPs to audit key controls

Using tabletop exercises to audit CASPs

Our Approach

1. Use **tabletop exercise techniques** for an interactive experience

2. Embed an **evaluation** of controls & reflection on **missing controls** into the exercise

- Define **exercise scenarios** reflecting the execution of selected CASPs by an attacker

- During the exercise, alternate:
  - (1) Incident **simulation, where participants must respond** and
  - (2) break-outs to reflect on possible security **controls improvements**;

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs

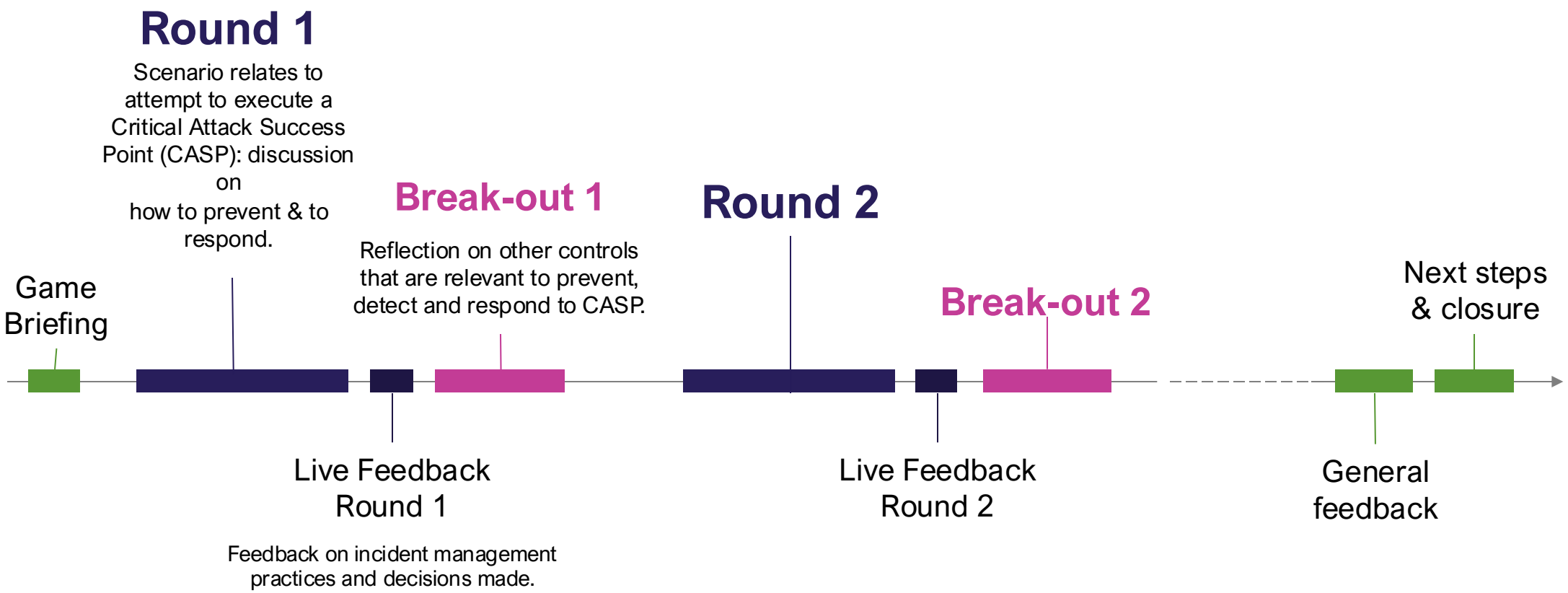
Our Approach

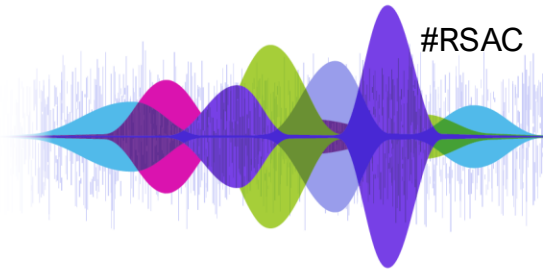
1. Use **tabletop exercise techniques** for an interactive experience

2. Embed an **evaluation** of controls & reflection on **missing controls** into the exercise

- **Pause** the exercise after each round, to **identify improvements**
- Prepare for this discussion, by pre-identifying **potential controls to** prevent, detect or respond to CASPs

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs


Round 1
Scenario relates to attempt to execute a Critical Attack Success Point (CASP): discussion on how to prevent & to respond.
Break-out 1
Reflection on other controls that are relevant to prevent, detect and respond to CASP.
Round 2
Break-out 2
Next steps & closure
Game Briefing
Live Feedback Round 1
Feedback on incident management practices and decisions made.
Live Feedback Round 2
General feedback



Using CASPs to audit key controls

Using tabletop exercises to audit CASPs

EXAMPLE

Example: exercising with Finance's Accounts Receivable team

- Tabletop exercise conducted with Accounts Receivable team of a global firm
- Focused on Fraudulent Invoices scenarios
- Covered the following CASPs
  - [A] Payment request from fraudulent e-mail domain
  - [B] Bank account change
  - [C] Fraudulent or negligent payment authorization

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs

Scenario featuring various CASPs

EXAMPLE

EXERCISE ONLY – CONTAINS FICTITIOUS SCENARIO INFORMATION

Jan 22, 2025
10:00

ROUND 1 | **Situation briefing**

nviso

BRIEFING

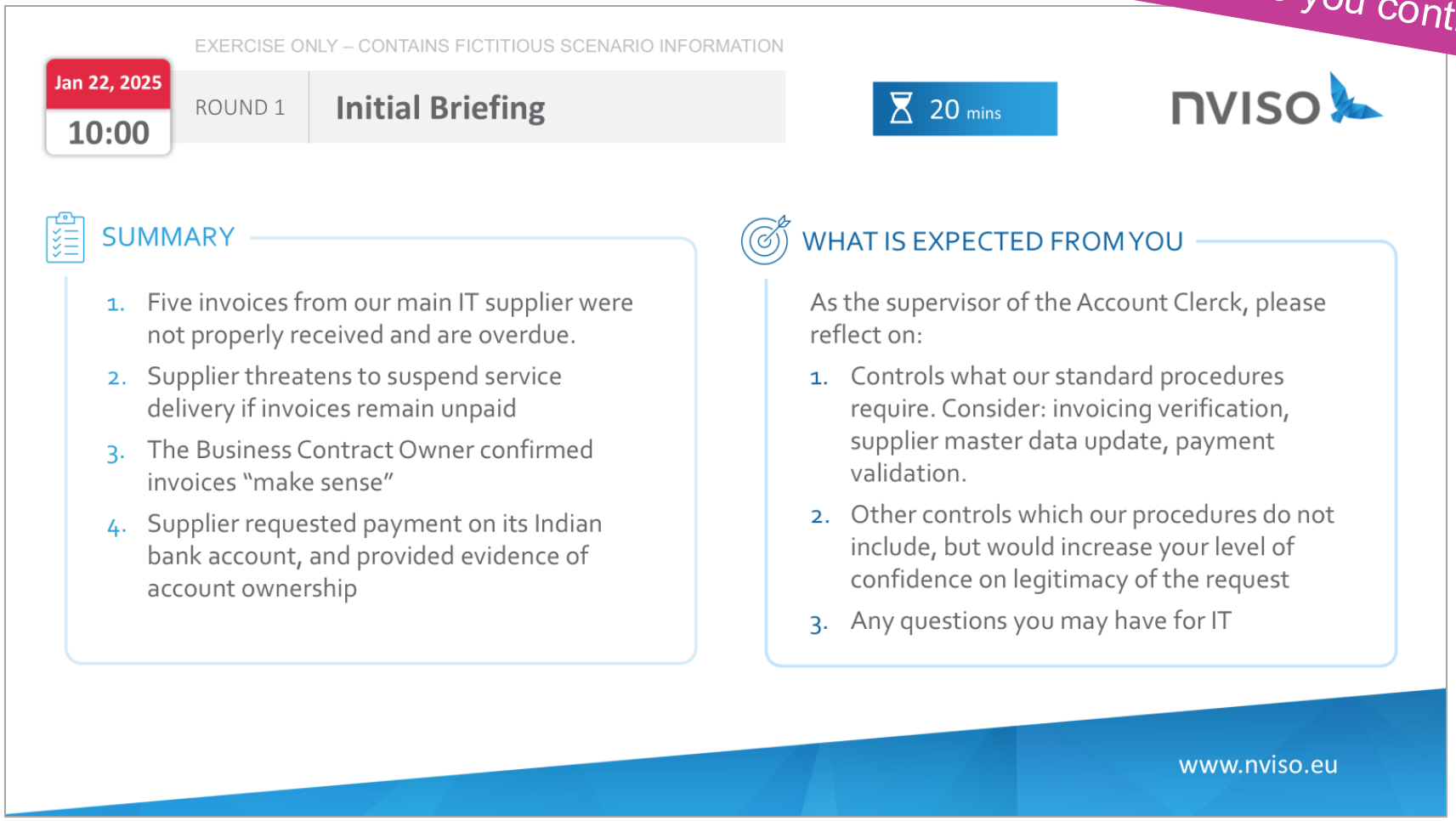
- A series of **overdue invoices** were received from Supplier A, our **main IT services offshoring supplier**:
  - The e-mail included an overview of **5 overdue invoices, for a total of 850k$** with a request to urgently proceed with payment, otherwise service will be interrupted.
  - The **e-mail** comes from our **usual Accounts Receivable clerk** at supplier side (James Bind)
  - The **invoices** look as the usually do, no surprise there
  - The e-mail includes, in attachment, a PDF copy of **13 e-mails** on the submission of the initial invoices and **subsequent payment reminders**.
- **Business confirms the invoices make sense:**
  - We have verified with the Business Contract Owner, who confirms that the invoices relate to 3 projects ongoing, involving 50+ staff, and on the critical path to delivery.
  - He wasn't aware they had been invoiced but **confirms that the number of MDs on the invoice is consistent** with the progress of the project.
  - You've checked, and we've paid up to 1.5m$ per invoice to this Supplier in the past.
- Given the late payment, the supplier requests to perform the payment **directly on the bank account of its headquarters, in India**.
  - This is a **new bank account**, that has not yet been created in our accounting system.
  - Your colleague responded to the e-mail, asking for a statement of bank account ownership, which he has received.

www.nviso.eu

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs

Tabletop discussion
"How do you control this"?

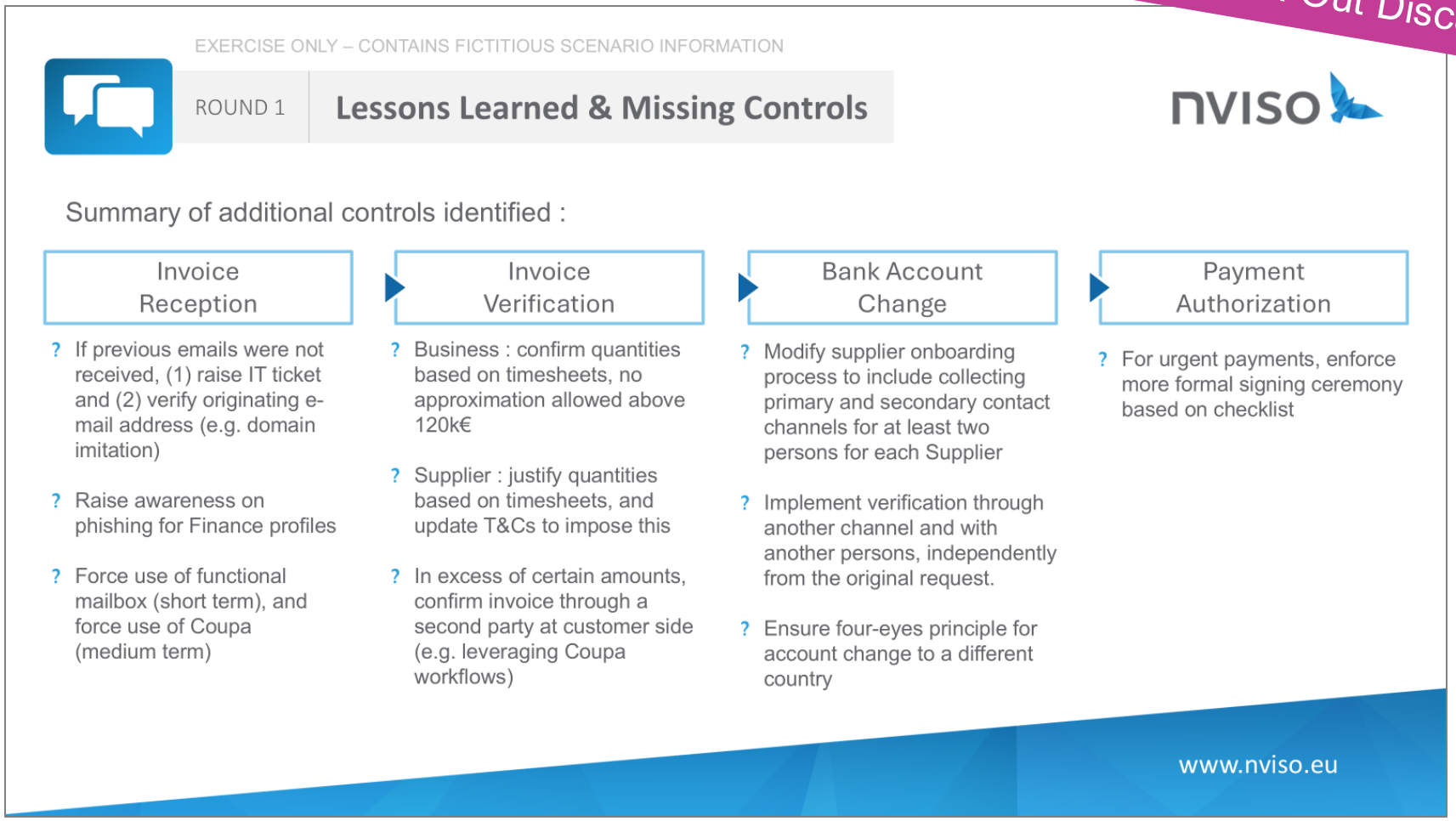
EXAMPLE


EXERCISE ONLY – CONTAINS FICTITIOUS SCENARIO INFORMATION
Jan 22, 2025
10:00
ROUND 1
Initial Briefing
20 mins
nviso
SUMMARY
1. Five invoices from our main IT supplier were not properly received and are overdue.
2. Supplier threatens to suspend service delivery if invoices remain unpaid
3. The Business Contract Owner confirmed invoices "make sense"
4. Supplier requested payment on its Indian bank account, and provided evidence of account ownership
WHAT IS EXPECTED FROM YOU
As the supervisor of the Account Clerck, please reflect on:
1. Controls what our standard procedures require. Consider: invoicing verification, supplier master data update, payment validation.
2. Other controls which our procedures do not include, but would increase your level of confidence on legitimacy of the request
3. Any questions you may have for IT
www.nviso.eu

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs

Outcome of Break-Out Discussion

EXAMPLE


EXERCISE ONLY – CONTAINS FICTITIOUS SCENARIO INFORMATION
ROUND 1
Lessons Learned & Missing Controls
nviso
Summary of additional controls identified :
Invoice Reception
? If previous emails were not received, (1) raise IT ticket and (2) verify originating e-mail address (e.g. domain imitation)
? Raise awareness on phishing for Finance profiles
? Force use of functional mailbox (short term), and force use of Coupa (medium term)
Invoice Verification
? Business : confirm quantities based on timesheets, no approximation allowed above 120k€
? Supplier : justify quantities based on timesheets, and update T&Cs to impose this
? In excess of certain amounts, confirm invoice through a second party at customer side (e.g. leveraging Coupa workflows)
Bank Account Change
? Modify supplier onboarding process to include collecting primary and secondary contact channels for at least two persons for each Supplier
? Implement verification through another channel and with another persons, independently from the original request.
? Ensure four-eyes principle for account change to a different country
Payment Authorization
? For urgent payments, enforce more formal signing ceremony based on checklist
www.nviso.eu

Using CASPs to audit key controls
Using tabletop exercises to audit CASPs

Tabletop exercises are also ideal to focus on a certain dimension, to ***improve certain specific capabilities***:

Focus on…	During exercise	During break-out
Detect controls	'How would you detect such CASP / attack step?'	'What other controls could be implemented to detect such a step? And: anything to improve on existing controls?'
Response controls	'How would you stop the attack, at that step?'	'Which other measures can we implement to stop such techniques? And: anything to improve on existing controls?'
Recovery controls	'How would you recover from the impact of the CASP, if successful'	'What controls, procedures, data and skills may be missing to (rapidly) recover?'

RSAC 2025 Conference

Testing CASPs
Sharing a few other interesting cases

A few success stories

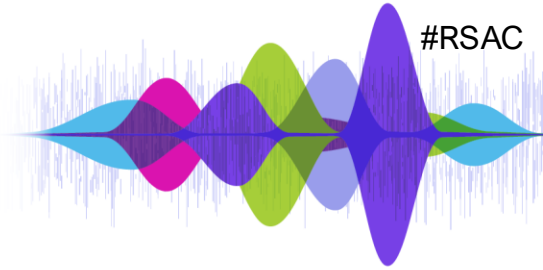
Some other interesting examples of how we've used CASPs:

- **Social engineer the Finance team**: stage attempts to request payment from AR clerks or other finance roles or business roles, towards a third party bank account (note: bank account may be blocked as part of fraud management, don't use your own ☺)
  CASPs: Supplier data management controls and Payment validation Controls

- **Hack customer onboarding process with deepfakes**: attempt to onboard customers or debtors through your system, leveraging false identities, identity documents or proof of identity (note: this may involve illegal activities, so legal advice is highly recommended to properly scope your tests).
  CASPs: Supplier data management controls

- **Forward mails from a certain mail address to your personal email:** attempt to create a mail forwarding rule to a domain you do not own (note: you do not want to introduce data leakage, so only forward mails from an external address that you own and fully control)
  CASPs: Detection & Blocking of Redirection

What will you start planning on Monday?



1. **Select two relevant scenarios** and perform the CASP analysis
   Hint: consider Ransomware & Fraudulent Invoices, they're 67% of the cases handled by the NVISO CSIRT over the last two years.

2. Start on a budget – and here are **3 ideas** already:
   - Organize a **tabletop exercise with your Finance team** on handling fraudulent payment requests
     Question: "Here is a fraud scenario, how would you have detected it?"
   - **Drop 'infected laptops' * at the helpdesk** and monitor their handling
   - Organize a **tabletop exercise with your Active Directory team**, focused on Recovery.
     Question: "How do we recover our AD following ransomware?"

3. Based on your CASP analysis, **define a testing roadmap** for the next 24 months

* Tip: don't really use infected laptops ☺

RSAC™ 2025 Conference

Q&A

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

For more information:

https://www.linkedin.com/in/vincentdefrenne/

https://www.linkedin.com/in/coenemichel/